Internet freedom, surveillance and censorship in the Middle East.

vgs4@kent.ac.uk | CO620 | 2015-2016

Abstract

This paper attempts to reflect on the state of surveillance, censorship, privacy and online activism in the Arab World[1]. The piece, as well as evaluating the general outlook of internet freedoms, focuses on the two nations with the highest amounts of surveillance, censorship and user rights violations, namely Iran and Saudi Arabia. It also examines Internet freedom in the aftermath of the Arab Spring by presenting case studies from Tunisia and Egypt.

The paper will also briefly address the implications of the western surveillance industry on the Internet freedoms of the Arab world.

Key Phrases : Censorship, Surveillance, Internet Freedom, Arab World, Middle East, Privacy, Online Activism, Arab Spring, Islamic Republics, Social Media, Politics on the Internet

---

[1] Includes the middle east and countries such as Libya, Egypt and Tunisia from the North African regions (MENA regions) with similar political and social structures.

Index

Preface

During the months of January and February, 2016 - I set about to write a piece titled, **"A Magna Carta of the Internet"**, of which the primary intention was to study the state of Internet liberties around the world, including the state of surveillance, censorship and the resulting behavioural patterns of Internet users. The concept, **"A Magna Carta of the internet"** was originally put forth by Sir Tim Berners-Lee in 2014, in an ambitious effort to identify and empower grassroots movements across the world to effect the local politic to maintain the internet as a free and open public space, devoid of surveillance or any form of censorship. [1]

An often heard criticism of the project was that the preservation of one's rights to an open, uncensored, neutral, and unmonitored internet could only be achieved as an ultimate result of a wider political struggle for privacy and democracy, and not through an à la carte movement whose sole objective is to separate the cyberspace from its political constraints[2]. While that argument is certainly true, the intention was to point out the lack of a wide interest in an explicit and specialised movement for an open cyberspace informed by context specific technicalities and principles.

I studied extensively in different regions of the world, the collective attitudes towards censorship and surveillance. Whilst there is a scattering of particularly encouraging pointers in form of localised grassroots movements fighting to achieve internet liberties [3], and gain constitutional awareness for censorship and privacy issues as well as free expression on the internet, there was very little empirical data that those movements would collate in their ambitions to form larger movements dedicated towards achieving Internet freedom, partly due to the inconsistency of key definitions regarding neutrality, privacy and censorship, and partly due to the Internet still being very much an emergent phenomenon in most parts of the world and peculiarly in the Arab world due to heavy political oppression[4].

The public opinion as to what societal and political functions the Internet should perform, how much oversight the governments should have over the national cyberspace[1], the acceptable extent of surveillance to preserve collective physical protection of the society, vary widely according to what part of they world they spring from and what particular time frame the surveys are conducted. [5]

In Western societies, where the World Wide Web has become a fairly integral part of both public and private lives of the citizenry, due to generally high penetration rates and relatively high democratic freedoms to access services and content - the debate concerning cybersecurity, censorship and surveillance is relatively vibrant and open and has recently taken a more spirited mantle, following key incidents such as Snowden revelations in the United States and the public objection to the Draft Investigatory Powers Bill in the United Kingdom to name a significant couple. [6]

In contrast, The Middle East offers a diverse terrain of democracies, monarchies, theocracies, stable regions, and regions in conflict. In a considerable number of these countries, the debate regarding Internet freedom is as important and vigorous as the struggle for democracy, due to the Internet being perhaps the only public platform whose complete regulation authorities find impossible.

---

[1] * National cyberspace, in this particular scenario should not be conflicted with a sovereign national cyberspace. National cyberspace is defined, for the purposes of this piece as :

I. A means of specifying the relative boundaries within which a state can exert its influence, through legislature, censorship apparatus or tangible infrastructure (when asserted in the extreme, and for the purpose of isolation, becomes a sovereign national cyberspace).

II. The accessibility and use of the internet, that is of concern to the populace of a given nation.

The Middle East houses some of the most connected countries in the world, that also happen to be among the most censored and most undemocratic. A number of countries in the region have also seen continued periods of instability as the region houses some of the most politically restrictive countries in the world. [7] The dynamic of the national cyberspace of these countries, as well as their censorship and surveillance apparatus, and the people's ambition to overcome these, forms the basis for an interesting study.

Methodology

Penetration Rates

The most reliable and widely used measurements are derived from either household surveys or demand-side data collected from ISPs. [8]

While the set of figures received from ITU (United Nations Specialised Agency for Information and Communication Technologies) is the most widely recognised, disparities arise in pieces of regional journalism when alternative data is obtained often from governments and ministries who tend to massage the figures, often quite optimistically.[9]

It is also worth mentioning that although not explicitly peculiar to the Middle East - extrapolative household online penetration surveys may not always result in particularly accurate assertions on factors such as the accessibility gender gap, or if connections are fast enough and usage is frequent enough to actually render any meaningful use of cyberspace.

For example, ITU figures identify Iran to be a comparatively less penetrative, but moderately equal cyberspace, where male to female online penetration ratio in 2013 was [33% male vs 25% female] *[2], whereas in highly connected Qatar, women take the lead with [97% male vs 99% female]. The almost equally technologically equipped and penetrative Saudi Arabia however (does not provide an ITU figure) from facts drawn from government sources, has a penetrative gender gap of [82% male vs 27% female].

Although this piece mainly relies on ITU figures for standardisation, it attempts to study how cultural, ethnic or societal disenfranchisements affect the penetration rate, and vice versa. For example, Iran's underground women's rights movement which gained momentum through social media[10], and the dissemination of information among Iraq's and Syria's Kurdish minorities amidst constant threats of terrorism and political marginalisation[11] point to the increasingly significant role that the internet will play as utility for achieving greater civil liberties, as the penetration rate of these communities increase. These communities are in most cases, the hardest hit, by the blanket censorship and surveillance apparatus of the state.

Qualitative Assessment of Surveillance and Censorship Reports

This paper is informed by a number of sources, and remains cognisant of the information provided by them despite not being directly referred to in the body. They also form the basis of a number of assertions. The paper takes into consideration, sources generated no later than December 2015.

The Freedom House- Freedom on the Net index is referred to as an overview of the general climate of the region, the scoring system maintained by Freedom House provides a generalised, but well informed bird's eye view of regional barriers to entry and violations of user rights. *US State department* reports are similar in their ambition – and provide a curation of the legislative and constitutional boundaries in each country.

The *Open Net Initiative* has halted producing regional reports since 2010, but nevertheless provides well framed assessment criteria of regional surveillance, and in depth insight into the state of censorship and surveillance leading up to the Arab Spring. Reports by *Privacy International* and *The Electronic Frontier Foundation* complement ONI reports by providing more up to date regional reports.

Reporters Without Borders publishes an index, titled "*Enemies of the Internet*", of which the two

[2] As in male internet users per every 100 males

regionally critical players, Iran and Saudi Arabia are discussed extensively in this piece. Reports by Human Rights Watch carry news articles and reports on violations of user rights, and the extent of freedoms enjoyed by netizens and journalists in different parts of the region.

The publications above are useful due to the difficulties in obtaining first hand information from most states in the region, particularly in a way that would be voluminous enough to draw accurate assertions – however, browsing around in social media reveals forums and chatrooms whose discussion elicits the general attitudes towards self-censorship and general subjects approached.

For example – despite many restrictions and atheism being declared a form of terrorism in Saudi Arabia[13], several Facebook pages are stealthily operated by the irreligious community – from within Saudi Arabia, these observations – whilst far from being accurate journalistic evidence – aid in penetrating the more generalised views put out by major sources mentioned above.

Additional research papers and publications will be mentioned where cited and in the reference list. Regional News reports are generally referred to, for further research and clarification – and will also be referred to where necessary.

●●●

A Brief Regional Overview

Acclimatised by a heavy presence of theocracies, dictatorships and absolute monarchies, the Arab world ranks as one of the least favourable places for online activism, yet due to the acute stranglehold most autocratic nations exert over their conventional media, the Internet has become an oasis for political and cultural dissidence.

The region offers diverse economic climates, from extremely wealthy to extremely underdeveloped - which has resulted in a wide range of penetration rates, with smaller nations such as Qatar, UAE and Bahrain boasting over 90% (ITU) of connected households, whilst a number of nations ravaged by years of war and conflict, such as Iraq and Libya have seen a hiatus in the development of ICT infrastructure resulting in poor penetration rates. [14]

Apart from a few countries such as Israel, Cyprus and to a certain extent Morocco and Lebanon, most countries in the region impose heavy surveillance and restrictions upon internet users.

Violations of these restrictions usually carry harsh legal penalties as well as in certain cases, has lead to extralegal harassment of users by authorities. [15]

Reporters without borders bestowed upon Bahrain, Iran, United Arab Emirates, Saudi Arabia and Syria, the unpleasant title, "Enemies of the Internet"[16], citing pervasive presence of censorship, surveillance and violations of human rights in reacting to dissident voices on the internet.

The Arab spring, whose cradle was social media and the online activist collective, had unfortunate consequences on the cyber landscape of the Middle East, from Iran to Saudi Arabia - the already vigilant and assertive government bodies smartened up, and found ways to crack down violently on online activism to deter the gestation of future mass protests.

After the Arab Spring, with the possible exception of Tunisia - most nations either have not seen vast improvements in privacy rights and freedom of expression, or in cases such as Egypt, the conditions have visibly deteriorated.

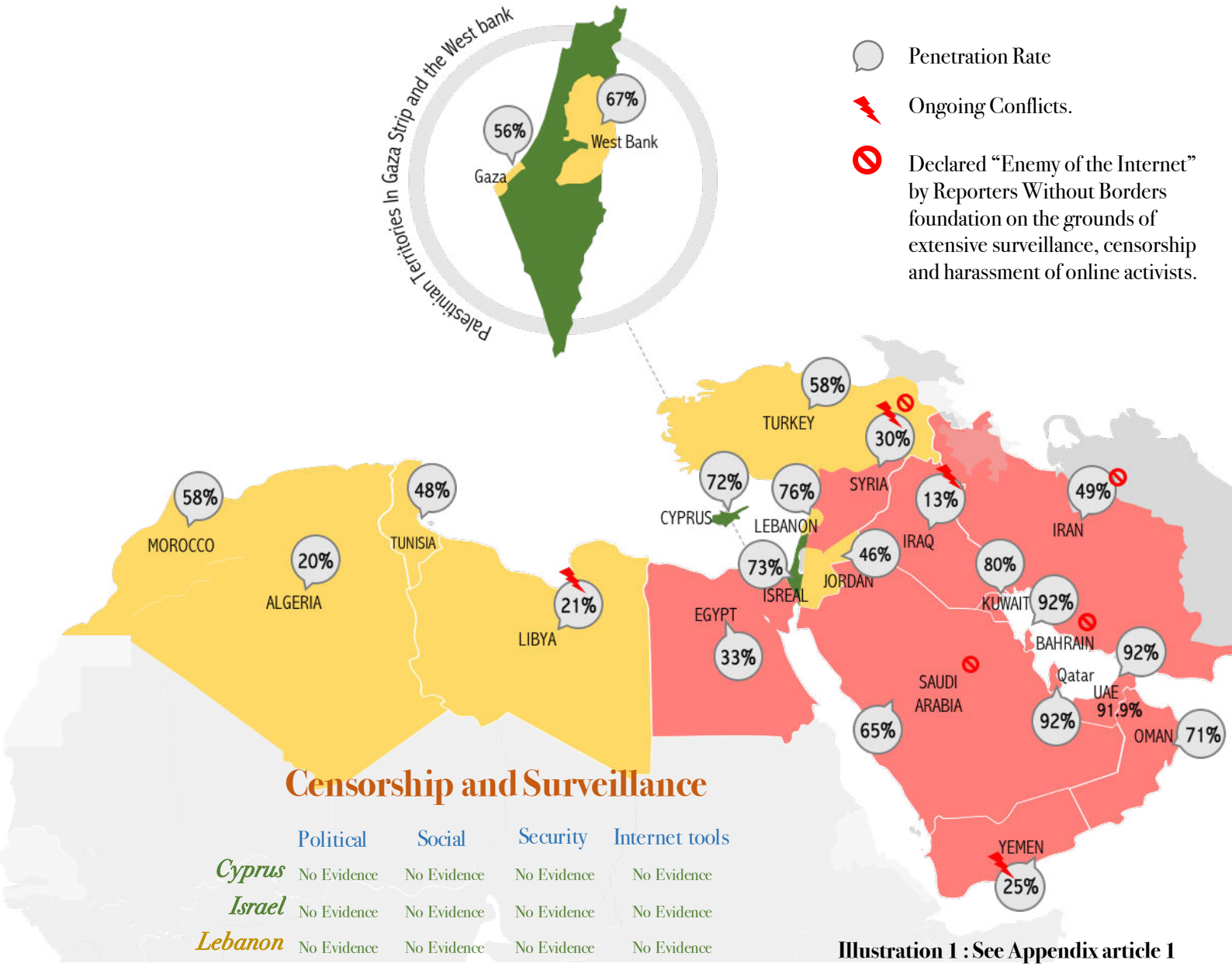


Illustration 1 : See Appendix article 1

Censorship and Surveillance

	Political	Social	Security	Internet tools
Cyprus	No Evidence	No Evidence	No Evidence	No Evidence
Israel	No Evidence	No Evidence	No Evidence	No Evidence
Lebanon	No Evidence	No Evidence	No Evidence	No Evidence
Morocco	No Evidence	Selective	Selective	Selective
Tunisia	Selective	Selective	Selective	No Evidence
Algeria	No Evidence	Selective	Selective	Selective
Libya	Pervasive	Selective	Selective	No Evidence
Turkey	No Evidence	Selective	Selective	Selective
Jordan	Selective	No Evidence	Selective	No Evidence
Gaza and the West Bank	Selective	Selective	Selective	Selective
Egypt	Pervasive	Selective	Pervasive	Selective
Syria	Pervasive	Pervasive	Pervasive	No Evidence
Iraq	Pervasive	Pervasive	Pervasive	Pervasive
Kuwait	Pervasive	Selective	Pervasive	Pervasive
Qatar	Pervasive	Selective	Pervasive	Pervasive
Bahrain	Pervasive	Selective	Pervasive	Pervasive
UAE	Pervasive	Pervasive	Pervasive	Pervasive
Saudi Arabia	Pervasive	Pervasive	Pervasive	Pervasive
Iran	Pervasive	Pervasive	Pervasive	Pervasive

Illustration 2 : See Appendix article 2

Surveillance and Filtering data extracted from research conducted by Open Net Initiative from 2006 - 2010.

Expands on reports produced by Freedom House (2010 -2015) with regards to Open Net Initiative's censorship and surveillance classification criteria.

Pervasive filtering indiscriminately targets large amounts of content within given categories

Selective filtering targets selected content within a limited amount of categories

Case Studies : Iran and Saudi Arabia, the two worst offenders in the region.

Iran : Slow, steady progress.

The Internet, or in its infant form Iranet, was introduced to the post revolution Iran in 1993, as a platform born into an already well defined set of cultural and political constraints. Dr Ai Larijani, the Director of Institute for Research in Fundamental Sciences of Iran sent Iran's first email in marking its introduction, and 1994 saw the first Iranian ISP, preceding a vast majority of regional nations. [20]

Iran′s political activism on the Internet predates the more commonly known Green Revolution and the Arab Spring. In 1997, Presidential Candidates Mohimmad Khatami and Ali Akbar Nateq-Nouri developed an Internet presence [21], complete with mailing lists and websites to compete against each other in winning over the then very small minority of elite, middle class Iranians who had been early adopters.

Internet played not very powerful, but a symbolically important role in the 1999 Student Uprising of Iran.[22] As authorities clamped down on public congregation, Iranian students tested the benefits of newfound technology to overcome the state barriers:

"The Internet has also become a powerful tool for grassroots democracy advocates, which in Iran have become synonymous with the student movement. During the summer of 1999, the Internet played an important (though limited) role in the uprising when Iranian students mobilised against the conservatives in chat rooms, organised meetings, interacted and communicated electronically, as the state continued to close down public places of political interaction."

(Middle East Review of International Affairs, Vol. 7, No. 3 (September 2003), Babak Rahimi)*

The trend continued in the 2003 protests against university privatisation[23], an observation of Iran's timeline of Internet penetration reveals the point at which the Iranian authorities had received enough indicators to consider the Internet a threat to Islamic code of conduct, and by extension, the ruling regime. By 2004, Iran had started to operate fairly low tech surveillance mechanisms on the internet. [24]

There is a particularly high volume of academic articles published on Iran's cyberspace dated around 2009-2010, the Green Revolution which sought to oust the hardline conservative president Mahmoud Ahmadinejad , largest of the kind since the Iranian Revolution of 1978 - was the first civil resistance of its kind to use the Internet in its modern context, which was acclimatised by particularly high use of modern social media and instant messaging. The culture attached to the internet use too, in its of memefication[3] political satire and audio visual content replacing text was never before observed in Iran.

Iranian cyberspace suffered heavily under the hardline conservative Mahmoud Ahmadinejad. The first ever comprehensive cybercrime law was introduced in 2009 [25], as a response to the Green Revolution, the vaguely phrased law gave the government the power to arrest, detain and maim members of the online activist community of Iran. A year later, all the major international social networking, content sharing and instant messaging sites were blocked [26], a precedent from which Iran has since failed to completely recover, 2011 saw an extension to the government censorship and surveillance apparatus in form of a state sponsored content manipulation and hacking base, called the Cyber War Centre.[27]

All of this, was compounded by Iran's extremely slow but also quite expensive internet connections. In 2013, 84% of Iranians were still using dial-up connections (UTI), and in fact Iran had the most expensive internet service in the world until key

3 Absorption of political content into the popular zeitgeist.

Key Events

2015

Iran saw a 1200% increase in its ICT ministry budget

Iranians defied a ban on content related to the reformist former president Khatami by setting up a mass social media campaign.

2014

President expressed wishes to ease censorship. and introduced a freedom of Information act, which enabled Iranians to access previously classified information from govt, authority websites.

An Iranian activist in exile launched "Stealthy Freedoms of Iranian Women" which gathered 170,00 followers in two weeks

2013

Authorities throttled VNP speeds discouraging their use

Ministry of communications expressed interests to create a "content refinery" for Iran. (1)

2012

Authorities throttled VNP speeds discouraging their use

2011

In verge of elections, Authorities blocked all encrypted international traffic for several days. revealing technologies for Deep packet Inspection.

Providing links to censored or banned content was made to carry a fine or imprisonment

Cyber Cafes were required to extract extensive personal information from clientele

Over 2000 officers were employed to manipulate pro government online content and carry out cyber attacks on online protestors .

2010

The government also reportedly allocated US$500 million for the purpose of combating soft protest and dissidence on the internet.

December 2010, all the major international social-networking and media-sharing websites such as Facebook, YouTube, and Flickr were blocked.

2009

June 2009 Saw the Iranian green revolution where mass protests were heavily aided by the user of social media and the internet to protest Mahmoud Ahmadinejad's reelection

Ahmadinejad's government enacted the Computer Crime Law, which gives the authorities additional power to survey and censor content that the government thought was unsavory.

[See Appendix article 3]

privatisation and expansion projects were deployed by the post Ahmadinejad government.

The Ahmadinejad administration deliberately axed the expansion projects for Iran's ICT infrastructure and imposed throttles in the already snail paced internet connections, in an attempt to thwart an atmosphere of critique and political opposition forming on the internet.

Progressive is a relative word, and by an excruciating stretch of the definition, the newly elected president Hassan Rouhani has been progressive, he has in fact been a centrist and a reformist whose key promises in the 2013 presidential election explicitly included the promotion of Internet freedom, and the reinforcement of Iran's crumbling ITC infrastructure [30].

Although grassroots social media movements, deployed by pro reformist Iranian youth have had a significant impact on the success of his election campaign against the hardliners, Rouhani has been unfaithful to the demands of those very same factions, despite Rouhani's insistence, genuine or otherwise in liberalising people's access to social media and freedom of information, the trajectory of censorship, oppression, state employed cyber attacks and intimidation has continued despite key improvements to infrastructure.

The Iranian National Internet [31], which has been in redevelopment since 2006 with the intention of allowing the state to be the sole curator of what circulates in the Iranian Cyberspace, includes as part of its endeavour to provide the Iranian citizenry with faster, cheaper and more secure access. Whilst the progress made by these initiatives has undeniably had an impact, without a political environment which preserves privacy and freedom of expression - technological progress becomes for the most part - meaningless, especially when these very advances double as utilities of reinforced surveillance and censorship.The rigour, efficacy, opacity and finesse with which Iran's revolutionary cyber police operates is of almost Orwellian sinisterness, and has the backing of Iran's supreme leader - whose power far supersedes that of the elected president Rouhani.

In 2014, the supreme leader issued a Fatwa against high speed Internet, deeming that high speed internet and 3G were against moral standards. The reason why such detail should be pointed out is to identify the sort of restrictions and the clerical mindset that impedes progress made by the moderates. [32]

Homegrown SSL (Secure Sockets Layer) certifications have been forced on the Iranian netizens , and the local industry or the few foreign services operating in the Iranian cyberspace are issued certificates of authorisation on the strict conditions that state, revolutionary guard and the military are granted pervasive access to the online activities of the users[33]. The state or the magnitude of censorship is not disclosed to the public, and attempts by activists to do so, such as FilterShod.ir[34] which collected and published data on mass censorship have been closed down.

Although the Rouhani administration has not made any breakthroughs, recent years have seen an easing of censorship policy, compared to the previous administration. Blocks and bans on encrypted services and social media have become nominal, and a vast proportion of Iranians have either Twitter or Facebook accounts, including government officials themselves.[35] The easing of sanctions following the Iran nuclear deal framework has opened up the economy with a visible influx of key services such as Apple and Android stores, Farsi language support for key google services, Xbox Live platforms and streaming services such as Netflix. [36] It should be expected that the authorities find ways to eventually close down the loopholes that these services may create in the surveillance and the censorship apparatus - but as matters stand in early 2016, the Iranian Cyberspace has had a breath of fresh air.

It also happens that more than half of Iran's population is under the age of 24 , one quarter of it 15 years or younger (World Bank Data), with a penetration rate of 40% [ITU] and still growing, partly due to the Rouhani government's increased stake in developing the domestic ICT infrastructure, and partly due to the removal of international sanctions against Iran which has seen an influx of technology and into the nation and a sense of optimism into its ether, the Iranian mindset is as proving to be relentless in their rebellion, ardent in the face of adversity, and innovative in their decent - and most importantly, patient and strategic.

The removal of sanctions will see improvements to Iran's Internet freedom, primary by enabling Iranians to use foreign SSL certificates[37], which will put the surveillance mechanism at a disadvantage by not being susceptible to backdoor in essential services. In an unprecedented opportunity Iranians will also be able to purchase server space abroad [38], which will restrict the amount of authority the Iranian government can impose over infrastructure. Being able to purchase authentic, secure software now means that Iranians won't have to use tampered bootleg versions which provide backdoor access to sensitive data.

Another positive indicator lies in Iran's industry, IT industry in Iran is growing at a rapid phase, and the startup scene in Iran has long since seized the attention of overseas investments [39], the marketplace itself has steered Iranian political interests to cut a compromise with its draconian censorship policies and allow a certain amount of freedom.

Iran is still one of the most repressive regimes in the region , but there are clear indicators to show that Iran is far from achieving a sovereign cyberspace without a heavy backlash from its netizens.

Saudi Arabia : Arbitrary and whimsical changes to the law.

The election of Saudi Arabia as the head of a key UN human rights council , was brow raising to even to those strongly cynical.

After all an absolute monarchy which criminalises political parties and national elections being at the frontier of a global collation for democracy and human rights, rather than validating the Saudi position, seemed to degrade that of the UN in the public mind, leading to outrage from many human rights activists and initiatives.

Saudi Arabia grants to its people very few liberties with regards to freedom of expression. With the royal family owning major stakes in the already heavily regulated press, where any criticism of the *Grand Mufti* or the any noticeable deviation from the Social Order is criminalised by law, writers, journalists, activists, artists, academics with the people at large, have sought refuge of expression on the Internet.

Proportional to both regional and world figures, Saudis are well connected - provided the fact that the county has the region's highest Twitter penetration of 2.4 million [40], partly explained by the youthfulness of the population where the majority of users are between 26 and 34, (World Bank Data) the ease of access, and even more compellingly due to the conventional media's extreme iron monotony of constant and virtually uniform rhetoric that only parts with extremely conservative entertainment to air customary praise to the House of Saud followed by more of the same old record from a hard-line cleric.

Although if one should draw an assertion from around the 150 million tweets [41] Saudis produce per month, social media seems most enticing due to the relative freedom of expression it offers, rather than accessibility.

"Because we are able to say what we couldn't say in real life. It's a breather from the suppression we live under, without fear," says one of the tweets. "Because it's the only democracy and made everyone talk - the rich and the poor, the prince and the ordinary citizen," is another. The tweets go on in a similar vein - perhaps best encapsulated by one of the most tweeted images showing a man whose mouth and eyes are covered, together with the words: "Because before the situation was like this." [42] (BBC article captures tweets from Saudi Arabia)

Social Media and the Internet has become a place of alternative opinion, political critique, congregation. Although the scorched earth treatment very much applies here too, the authorities, and also the political conservatives have understood the potential power of the Internet and have smartened up, propping up their own propaganda to compound into the already murky waters of surveillance, extreme censorship and of course, as we will come to discuss, the harsh penalties that activists are subjected to.

Surveillance is officially justified under vaguely defined Anti-Terrorism Laws [43], and the cyberspace is subject to heavy government agency. ID based Registration is required when purchasing mobile phones, and even topping them up. To curb the black market trade of unregistered sim cards, the regime has sought fingerprints conditional upon the purchase of a mobile voice or data connection, which will render the already tight space for anonymity, almost airtight. [44] Encryption was reported to be banned in Saudi Arabia, but recent provisions has made for commercial channels, state approved, [45] with licenses - of whose data protection will not extend to the wider public - but to the most part, enforcement of encryption is not thoroughly administered anyway as the government has begun to use a plethora of decryption and deep packet inspection tools to infiltrate encrypted transactions.

A considerable bulk of equipment and technology for Saudi surveillance is produced in the west,and as the penetration rate has increased, the authorities have been able to source a highly sophisticated surveillance apparatus capable of circumventing encryption and performing selective deep packet inspection. [50]

Key Events

2014	Govt. began to monitor YouTube videos produced in the country to ensure compliance with local laws. Sweeping anti-terror regulations introduced blanket laws that severely impeded internet freedom [1]
2013	Govt. Temporarily blocked thousands of twitter accounts. Several government ministries warned that tweets are monitored and employees may face termination from their jobs for expressing critical opinions.
2012	Government threatened to block YouTube over controversial "Innocence of Muslims Video", which was eventually blocked. Government Passed : Those who forward or, retweet IM messages that violate the sanctity of public morals, religious values and public order, will be sentenced to five years in jail. New Law made ID number conditional in recharging prepaid mobile cards.
2011	Millions took to social media in an unprecedented elevation in online activism demanding social, political, and economic reforms. Legislation was passed to license online news outlets.
2010	The government expressed interests that bloggers were issued government licenses. Services for Blackberry Mobile's IM service was banned, due to encryption, the ban was repealed after government obtained means to access encrypted data with support from BB.
2009	Ministry of Interior Mandated Cyber Cafes to install Hidden CCTV Cameras and operate under tight curfews. **[See Appendix Article 4]**

Italian based cyber security company - Hacking Team, has provided extensive surveillance technology to the regime [52] , there are also widely verified reports of the very same censorship tools such as German owned FinFisher and American owned Blue Coat's appliances being used for blanket surveillance, some intermittently deployed at times of political tension, others, contingent in the background.

The State employs extensive manned surveillance agents across multiple social media sites. [53] Their function in spying is compounded by seemingly spontaneous, but well organised humiliation and threatening campaigns against activists as well as widespread content manipulation and propaganda in favour of the House of Saud.

Another threat to privacy and the freedom of expression in Saudi Arabia is the NSA's active relationship with the Saudi Arabian Surveillance agencies. Edward Snowden produced an extensive memo in April 2013 [54] which outlined the vaguely framed provisions on "analytical and technical support" to the Saudi Internal Security by the US state department.

The complete excerpt, at a glance has very little specifics on the exact nature, deployment strategy and the coverage of NSA surveillance assistance, it is also not clear, nor has been explained by the office of national intelligence as to what interpretation of internal security the document alludes to.

A relatively benign interpretation of said intelligence would be intelligence related to terrorism in Syria, and the active recruitment of young adults as fighters which is rampant and is of genuine concern, but Saudi Arabia's own interpretation of state security involves the sanctity of the state religion, elimination of all possible critique of the royal family, any form of religious dissidence, or inclusively, any deviation from the public order.

As far as the Saudi Regime has been concerned the reinforcements involving the NSA have been channeled towards stifling extremism and terrorism in the country, but then again, Saudi

Arabian terrorism law, and the very definition of terrorism is extensive, vaguely defined, and is used as blanket excuse in numerous occasions to thwart dissidence.

"Any act carried out by an offender in furtherance of an individual or collective project, directly or indirectly, intended to disturb the public order of the state, or to shake the security of society, or the stability of the state, or to expose its national unity to danger, or to suspend the basic law of governance or some of its articles, or to insult the reputation of the state or its position, or to inflict damage upon one of its public utilities or its natural resources, or to attempt to force a governmental authority to carry out or prevent it from carrying out an action, or to threaten to carry out acts that lead to the named purposes or incite [these acts]."[57]

Perhaps the single strongest case that has come into wider public attention in recent times in the case Involving Raif Badawi, whose Facebook page, Saudi Liberals – saw his arrest after gaining popularity among a considerable number of Saudi youth, and subsequently his lawyer – for the crime of defending his client.

Surveillance seems to have actively discouraged the country's Shiite minority in asserting their rights to freedom of congregation and religious expression, as increased connectivity comes with increased traceability – the religious and racial minorities of Saudi Arabia (not unlike in Iran) resort to an extremely self-censored, minimal presence.

The country's female population too – heavily marginalised in the cyberspace with an extreme disparity of 27 per 100 women on the internet compared to 82 per 100 men, (ITU) but in an interesting twist – the majority of bloggers in Saudi Arabia happen to be women. [59] Heavy surveillance and harsh punishments for the violation of the status quo has acclimatised the Saudi cyberspace to a culture of self censorship – therefore women bloggers for the most part pass time chronicling their daily lives in numerous blogs and social media posts in carefully chosen language. The primary reason for the extremely high number of female bloggers appears to be female unemployment, as only 6% (World Bank) of Saudi Women work, as of 2015.

The internet has, in this instance challenged a major facet of the status quo regarding women. The reason why women are barred from driving in Saudi Arabia is an extension of a culture whose intention is the isolation of women from would be unsavoury evils of the society*[4], such as non segregated environments, and men who happen to be strangers (Freedom House) . The Internet is as non segregated and public as it could be, the symbolic importance of being able to broadcast opinion to the wider public has never before been so commonly and so accessibly enjoyed women's right in Saudi Arabia.

"In Saudi Arabia, we live more of a virtual life than a real life. I know people who are involved in on-line romances with people they have never met in real life ... And many of us use Facebook for other things, like talking about human rights and women's rights. We can protest on Facebook about the jailing of a blogger which is something we couldn't do on the streets"[61] (Freedom House, name of the quoted blogger undisclosed)[5]

The lack of any democratic power structure even compared to Iran, and a culture of impunity that has resulted in vaguely defined, constantly changing laws and regulations in reality puts Saudi-Arabia in a worse position than Iran.

Whereas Iran is pacing slowly towards achieving greater internet liberties by exploiting the very limited democratic features afforded to them by the constitution and state legislature, the Absolute monarchy of Saudi Arabia has to depend solely on arbitrary progress, made often by the good and gentle will of the monarch.

---

4 Paraphrased. After years and years of crackdowns on persistent female activists, the kingdom might consider taking a more moderate approach in tackling women's issues. At the time of writing - the removal of restrictions for women drivers is being debated

5 Extracted from freedom house, Identity of the quoted unknown, but verified to be authentic refer to (http://www.columbia.edu/itc/sipa/nelson/newmediadev08/Why%20Saudi%20Women%20Blog.html) for a descriptive note.

The Middle East and the Surveillance Industry.

State operated surveillance and censorship apparatus across the MENA regions are rarely home grown, as needs arise in tackling the ever growing online user base - authoritarian regimes often look to the west, as potential clientele of a multi billion dollar surveillance industry.

There have been numerous incidents, scattered throughout the Middle East, of human rights activists, journalists and dissidents, being shown as prosecution evidence, their own private emails, text messages and other private communications whilst being in custody. Countries from Saudi Arabia to Qatar are able to perform deep packet inspection of private content, holding them as evidence, in many cases for politically motivated prosecutions.

The ethical and moral issues that arise in allowing US and European companies to sell surveillance equipment, train surveillance units and aid the process of curbing free speech and the advance of human rights in authoritarian regimes are well documented, but seldom tackled in a meaningful and effective manner.

While Saudi Arabia has long since purchased surveillance equipment from companies the United States and the UK. Iran has turned from Europe to China [62] as the main source for surveillance equipment. The lack of transparency in transactions made with countries such as China, leaves the activist community with very little knowledge about impending developments to the surveillance machine.

In an interesting turn of events, in 2011 an Israeli company's deal with a Danish redistributor, unbeknownst to either party resulted in products being routed through a middle man to Iran [63], a nation that has called for the annihilation of the Jewish state. There is a surprising number of cases where companies are quick to distance themselves from the sale of a product which either invalidated an embargo, or was scandalously involved in a major human rights violation, such as Blue Coat's case in Syria's Assad Regime - as the company was accused of both.

During the height of the Arab Spring in 2011, the Assad Regime engaged in a brutal crackdown of online activists, which saw numerous cases of imprisonment, assassination and harassment. One of the key surveillance apparatus used was manufactured by Blue Coat, an American multinational. The appliance provided the Assad regime the capability to perform extensive filtering, deep packet inspection and decryption of SSL-encrypted content, which compromised the security of a number of journalists, online activists and protestors.

Blue Coat admitted to their products being used in Syria, as Syrian sources too confirmed - but denied any knowledge of transactions with Syria citing that products, originally marketed to Iraq may have been routed to Syria through Dubai via a third party distributor named Computerlinks.

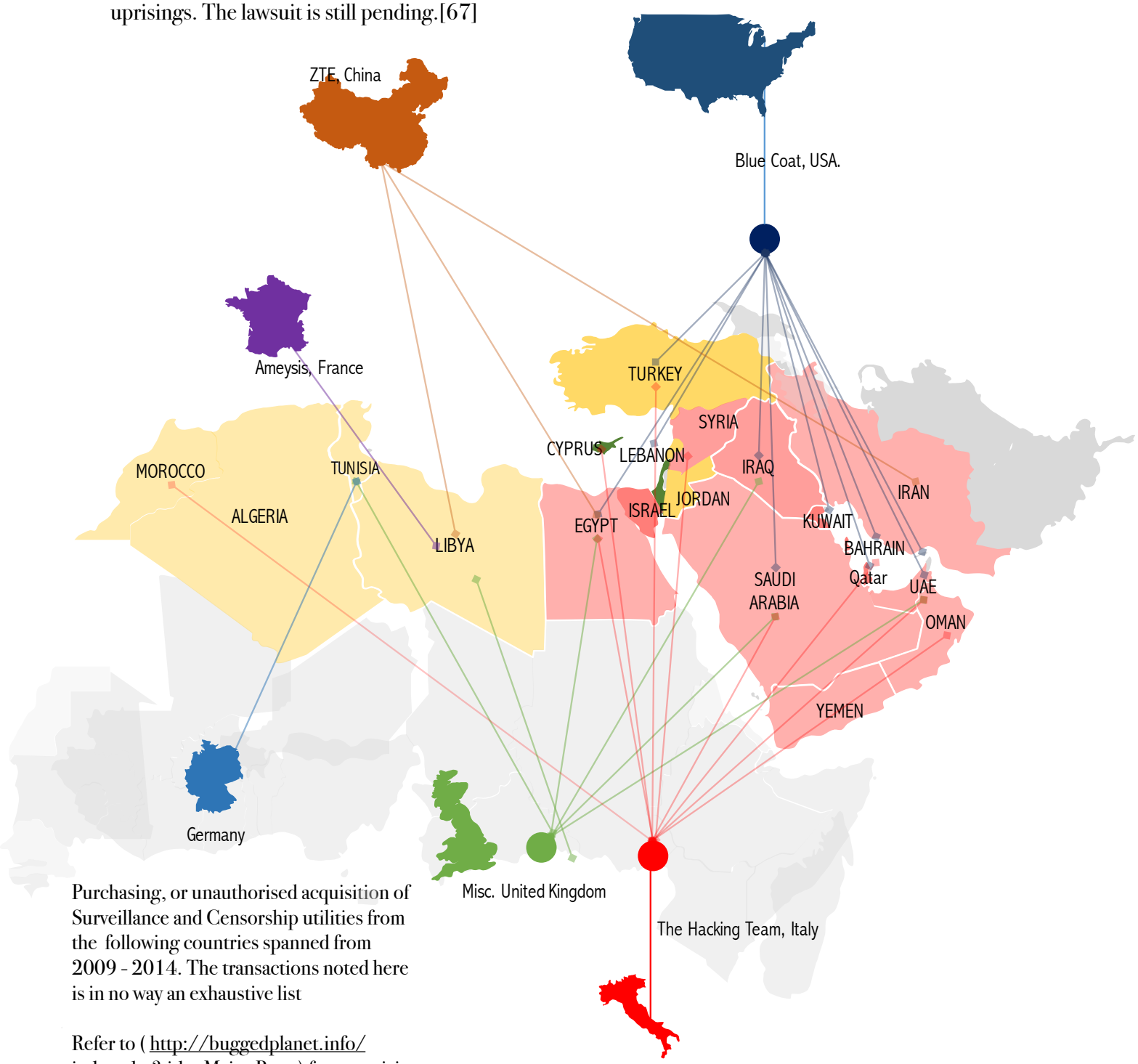
Although stolen software, or genuine security software repurposed as surveillance equipment by malicious agents is not an entirely unbelievable excuse, given the complexity of the operation of certain surveillance products, as well as news of those accused of theft receiving updates, and the fair amount of support that is required from the vendor in the initial installation of these systems, raise doubts. However Blue Coat, having supported the investigation, were made exempt from any charges of disrupting the US embargo with Syria. [64]

But as often in these cases, it is not the possible violation of embargoes that is of concern to most internet activists and the human rights community, but the sheer disregard of the moral and ethical implications of selling surveillance equipment to regimes, who are known violators of human rights. As Electronic Frontier Foundation stated :

"Blue Coat's blatant lack of concern for human rights is alarming. There are far more repressive regimes in the world than there are embargoed countries. Several United States allies, including Bahrain, Saudi Arabia, and Qatar, are also using Blue Coat systems for censorship and surveillance. But Blue Coat is surely

unconcerned; after all, exporting to those countries isn't against the law; it just helps violate the human rights of the people living under those regimes." (Julian York EFF) [65]

Companies from a number of European nations, including France, United Kingdom and Germany, traded with authoritarian regimes before the Arab Spring. [66] The French corporation, Amesys is currently under a lawsuit brought forth by International Federation for Human Rights (FIDH) for complicity in torture during the Libyan uprisings. The lawsuit is still pending.[67]

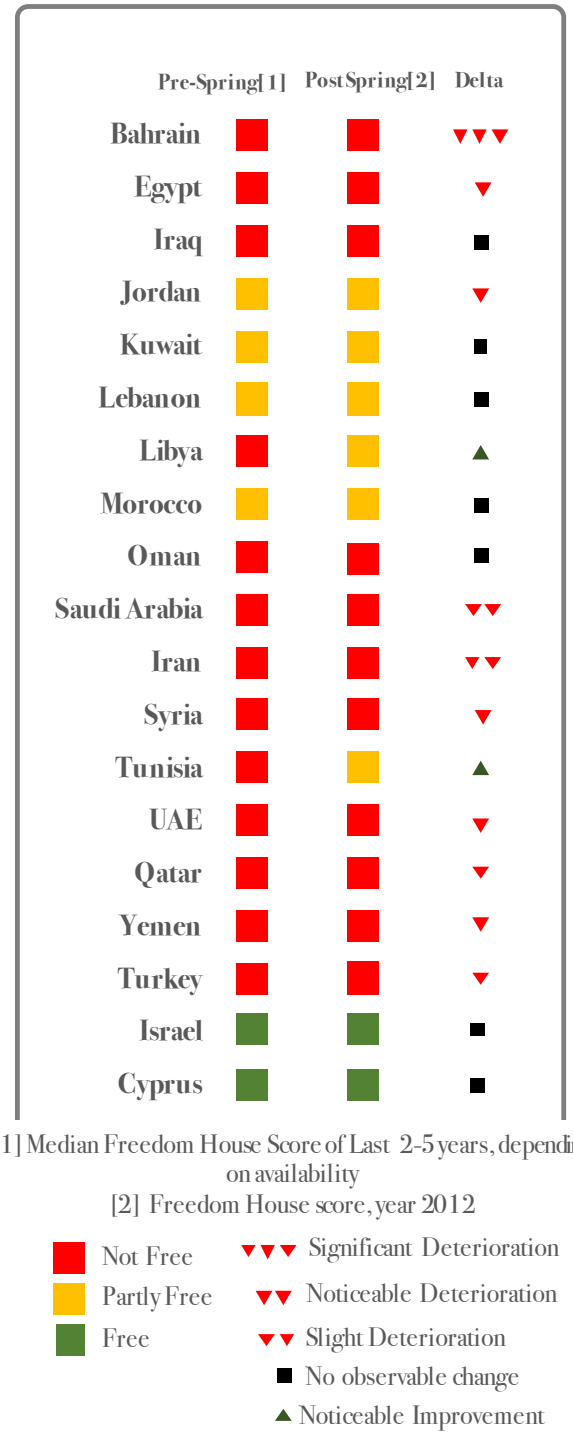


Purchasing, or unauthorised acquisition of Surveillance and Censorship utilities from the following countries spanned from 2009 - 2014. The transactions noted here is in no way an exhaustive list

Refer to (http://buggedplanet.info/index.php?title=Main_Page) for an activist maintained wiki of surveillance equipment transactions.

Despite being recognised as Dual-Use goods, capable of being used for defensive as well as offensive purposes by the Wassenaar Arrangement, [68] the unethical sale of surveillance software to abusive regimes continues.

Privacy International, and Human Rights Watch - have brought forth numerous appeals to both the US and EU governments to make surveillance service providers responsible for a collective ethic that deters the provision of custom to potential human rights violators - but these complaints have garnered only statements of solidarity and lukewarm responses - In short, the trading of surveillance equipment to oppressive Middle Eastern regimes continues.



The Arab Spring : Before and After

There is a diverse debate about the impact of the Internet and the social media on the Arab Spring. Some say that the use of Internet in communicating political dissidence, and as an aid to planning, congregation and canvassing is inconsequential and would even undermine the actual thrust socio-political unrest which caused the 2011 upheavals.

First, that despite their status as exciting new tools of political mobilisation (and exciting new subjects of behavioural research), social media and Internet connectivity are probably not important causes of the Arab Spring; [...] while we cannot conclusively and definitively establish the relevance of any of these factors,(Chonghyun Christie Byun PhD and Ethan J. Hollander PhD, 2015) [69]

Whereas others, and more in number have contrasted uprisings of this nature with historical parallels and explicitly validate claims that the Internet, to a certain extent was a remarkable catalyst in the revolts.
"[..] they all happened at a time in which advances in communication technologies, in particular the Internet, allow for a much faster circulation and dissemination of information. Hence the constant association of these revolts with Twitter, Facebook, YouTube, etc.

Indeed, one of the main explanations emerging immediately after the Iranian uprising of 2009 and the Arab revolutions revolves around the role of new technologies in provoking these movements. By associating these revolts with new technologies—phrases such as Twitter revolution, Wikileaks revolution, Facebook revolution—not only pointed out the potential of new technologies but more

significantly seemed to claim that such tools were the main engine and agents of socio-political change in the region. This is a certain amount of truth in that explanation. Imaginative use of new technologies to disseminate information, to focus the collective minds of populations, to break down the barriers of censorship and to pave the way for the emergence of a 'public', was real, and not simply a figment of western journalists' imagination. Many activists in Iran and the Arab world also articulated and forwarded such interpretations of events in the region. (Arab Revolutions and the Iranian Uprising: Similarities and Differences
Khiabany, Gholam) [72] "

Perhaps a more detailed academic distinction should be made about the terminology, causes should not be confused with mobilisers. As the article will elaborate, online activism has certainly had a clear mobilising effect in the Arab Spring. While upheavals against theocracies, dictatorships and kleptocracies have risen before, this would be the first instance that the public and the academic circles alike, get to study and experience the involvement of the cyberspace in a new dimension to protest and dissidence, an extremely robust and adaptable non tangible medium whose facility in content duplication, distribution, agility and public-broadcasting has been unparalleled, and would certainly warrant more academic exposure.

Also, any claim that the cyberspace is of little relevance to modern dissidence should be reexamined following the swift moves of Arab nations to develop extremely costly surveillance reinforcements, increase censorship in most cases by an order of magnitude and introduce new laws which facilitate the indiscriminate clampdown on activism in the immediate aftermath of the Arab Spring - indicating the realisation by those regimes who felt the tremors of 2011, of the significant effect of social media as a catalyst in political change, and a conduit of dissidence.

A more centred compromise between the two positions would be cognisant of the fact that Internet and social media whilst not necessarily are causes in themselves, are extremely relevant.

The Arab Spring emphasises the role of the Internet as a mobiliser and a catalyst in political activism by serving as an alternative broadcasting platform championing in people journalism, in a region where conventional media operate under extreme limitations.

●●●

Case Studies : Tunisia and Libya, Internet after the Arab Spring.

Tunisia : A success story.

Tunisia, which was the epicentre of the Arab Spring, is perhaps the only country that achieved a successful and significantly impactful transition from an autocratic regime of 11 years to a relative democracy.

Internet was introduced to Tunisia in 1996, during the Zine El Abidine Ben Ali administration. First broadband connections were established in 2003, and the penetration rate grew over 36% under the state owned telecommunication service until 2010. (ITU)

The Ben Ali Administration which spanned from 1989 to 2010 - saw a state censorship and surveillance apparatus systematically growing in technical competency and coverage. Tunisian media, which has been reasonably free and democratic in the early quarter of Ben Ali administration, suffered increasingly heavy restrictions leading up to the Arab Spring years. [74]

Vague laws citing national security, libel (and even specific ones which made offensive statements about the president carry prison sentences of up to

five years) [75] and defamation as well as extralegal harassment, vandalism, destruction of property and outright censorship of television, radio and the press saw a rising number of Tunisians subscribing to Social Media for political discussion, congregation and information.

Censorship and surveillance was at their highest in the three years prior to the ousting of Ben Ali, and those efforts affected not only online journalists, but also their subscribers. Cyber cafe users had to register their personal details before being given access to service. Social Media, and video distribution sites were routinely blocked by government and local blogs and news websites were frequently blocked, or hacked. [76]

2009, to 2010 reports from OpenNet initiative cited that Tunisian censorship apparatus was pervasive to the extents seen in China and Iran, [77] the country mainly utilised SmartFilter by McAfee to conduct mass surveillance (The product is now owned by Intel). Phishing attacks were common and regular breach of private email and social media accounts were quite prevalent.

An article written for the Atlantic quotes from the pro revolutionary head of the Tunisian government who discovered the previous regimes surveillance equipment :

"I had a group of international experts from a group here lately, who looked at the equipment and said: 'The Chinese could come here and learn from you.' (Post Ben Ali Head of the Tunisian Internet Agency Moez Chakchou, quoted in article by EFF) [78]

There were no constitutional justifications to the state of censorship or surveillance in Tunisia, unlike in traditionally Islamic nations, no particular attention was paid to religious dissidence or critique, therefore, once the Ben Ali Administration fell in 2011, the transition to sparse surveillance and minimal censorship of content was achieved with relative ease.

During the Ben Ali administration, all of Tunisia's internet traffic was channeled through a single gateway controlled by the Tunisian internet Agency. Pornographic content, content critical of the prevailing regime, information on the state of human rights in Tunisia as well as any mechanisms to circumvent existing censorship apparatus were prohibited– self censorship was prevalent in the mainstream of widely consumed online news outlets and magazines whereas deeper, more dissident critique was limited to more obscure blogs and social media groups – which were being discovered and brought down in a cat and mouse game led by authorities. In 2013, Tunisia passed a decree law that afforded online journalists and news outlets with many of the same rights traditional journalists enjoy [80]

The single gateway of the TIA, and the singular backbone to the Tunisian cyberspace thereof, was weakened in 2013 with ISPs bypassing TIA and accessing international networks directly. [81] Furthermore, in 2014 Tunisia's first privately owned submarine fiber-optic cable was inaugurated, further easing the dependency upon state infrastructure. [82]

Egypt : Internet freedom in decline.

In 2011, protesters filled the Tahrir Square in Cairo to demand the resignation of Hosni Mubarak, the Egyptian president since 1981. Victorious in their protest, the Egyptian people elected Mohamed Morsi, the first ever Egyptian president to be democratically elected into house.

Only a year later, Tahrir Square saw masses of protestors again, this time demanding the resignation of Morsi, who had abused the powers of his short lived presidency. Following a military coup d'état, bloodshed and chaos, Egypt's army chief general Abdel Fattah el-Sisi was subsequently elected as Egypt's 6th president.

Egypt has descended from a kleptocracy to a dictatorship, and the relative freedom to use the Internet as a means of dissidence and a utility for democracy has declined. Egyptians are confronted with a state surveillance and censorship apparatus that is growing in both complexity and coverage.

Egyptians realised the potential of the internet, as a platform for dissent in its full force in 2011, despite a relatively low penetration rate of 33% (ITU), the

Egyptian youth used social media to mobilise, inform and empower the wider community into protesting the Mubarak administration. Amidst the blockage of traditional media routes through which to disseminate information about the extent to which the Mubarak administration clamped down on protests, Egyptians took to the internet - informing fellow protestors and international media through the wide circulation of videos and photos.[83]

Along with Libya and Syria, Egypt was one of the few nations to see the complete severing of its connections with the outside world, as the Mubarak administration deployed what is now more commonly known as a Just-in-time blocking strategy, which at the apex of public protest - ordered to shut down, denied power to, or administered surgically orchestrated sabotage to all but one of the country's ISPs.

Dyn Internet Intelligence (Formerly Renesys) Internet outages bulletin noted and documented the 2011 events, and commented :

"But every Egyptian provider, every business, bank, Internet cafe, Web site, school, embassy, and government office that relied on the big four Egyptian ISPs for their Internet connectivity is now cut off from the rest of the world. Link Egypt, Vodafone/Raya, Telecom Egypt, Etisalat Misr, and all their customers and partners are, for the moment, off the air." [84]

Following the ousting of Hosni Mubarak, both the transitional legislature and the later introduced national legislature during Morsi administration, accommodated heavy demands from Egyptians for unfettered, uncensored internet access and fair treatment of bloggers. This was mostly done to appeal to the fervour of the considerably large number of Egyptians who expressed the need for freedom of expression both online and offline. They had rallied and campaigned to oust Mubarak, and had been subjected to considerable harassment by the authorities for their activism during the Arab Spring.

Before the political restlessness that resulted in the Arab Spring, social media users and bloggers had enjoyed fairly unrestricted access to the internet, blogs and news sites, including even those that harshly criticised Mubarak administration. Freedom House reports from 2008-2009 categorised Egypt's internet as being partly free.

Even though the Mubarak administration engaged in low level surveillance, intermittent censorship and had engineered the internet infrastructure and the country's fibre-optic cable network into a centralised, highly controllable framework which allowed the authorities to have a restrictive chokehold [87] on resources when needed, the only practical use of those facilities were unobserved until the 2011 blackout.

The internet was the primary platform in which disobedience to the prevalent social taboos regarding sensitive issues such as religion, and critique of the administration flourished, in fact online activists transcended the blogosphere to mainstream media celebrity, and claimed awards for Journalism - sparking ambitions for online activism in the mainstream populace [88]. Online activism was a key force in persuading the Egyptian people to rally against the 20 year Administration of Mubarak.

After the ousting of Mubarak in 2011, the interim Supreme Council of Armed Forces, now with a deeper understanding of the power of the internet, in addition to maintaining the surveillance apparatus of the Mubarak regime, continued to implement new, modern surveillance mechanisms, despite which authorities understood the role the internet played in crafting public opinion and began to engage with the public online. Soon, the Egyptian cyberspace appeared to be an active platform for real time political debate with the state, emerging political parties, the military and the people. Yet the new surveillance apparatus continued to operate in the background, collecting information on key activists and political figures for posterity, but once the people saw through many of the content manipulation tactics of the SCAF and increased the rigour of their critique, the surveillance and censorship quickly became overt and intrusive.

Until 2010, the surveillance and censorship mechanism of the Egyptian authorities were fairly relaxed, in fact they were far more open, and permissive than those of its Arab neighbours, particularly due to the secular nature of the

governance, the transfer of power to president Morsi, which saw the power structure shift from secularists to the Muslim Brotherhood resulted in an increased number of cases pertaining to censorship, particularly of those material which sought religious critique. The new regime also put forth a ban on websites containing pornography, similar proposal rejected by the supreme court on two prior occasions during the Mubarak administration was passed in 2013, circumventing any judicial intervention. [89]

The 2014 Egyptian constitution, as well as the interim constitution of 2012, guarantees the citizens right to privacy, and makes it legally binding that any surveillance or spying has to supersede explicit court orders.

The post Mubarak surveillance mechanisms, both under Morsi and el-Sisi have been in breach of the reformed Egyptian constitutional rights on privacy.

In 2012, the Morsi administration sought Iranian advice on improved surveillance capabilities [91], and in 2014 the el-Sisi administration in a move that drew criticism not only from privacy activists but also pro government media, announced a tender for equipment and technology capable of conducting surveillance on social media and instant messaging services including Viber and WhatsApp [92]. It was discovered in a 2014 report that the authorities were developing the language capabilities of these apparatus to include both colloquial and classical Arabic. [93]

The impending predicament of the Egyptian cyberspace is perhaps best contained in this translated excerpt from the tender calling for Social Media surveillance equipment.[6]

"Despite the various benefits and many positives of human interaction on such networks, on individual and communal level, there are also many negatives and dangers coming out of them, to the extent of threatening the safety and stability of society, especially with the increased effect of the Internet and social networks, where news travels without borders or limits, where democratic principles are grounded, and with short time available to make decisions to face societal crises, in addition to several variables and factors affecting the state of security. Security agencies are facing new problems, and external variables are affecting the state internally. Destructive ideas published on such networks are increasing, most importantly: blasphemy and skepticism in religions; regional, religious, racial, and class divisions; spreading of rumors and intentional twisting of facts; throwing accusations; libel; sarcasm; using inappropriate words; calling for the departure of societal pillars; encouraging extremism, violence and dissent; inviting demonstrations, sit-ins and illegal strikes; pornography, looseness, and lack of morality; educating methods of making explosives and assault, chaos and riot tactics; calling for normalizing relations with enemies and circumventing the state's strategy in this regard; fishing for honest mistakes, hunting flesh; taking statements out of context; and spreading hoaxes and claims of miracles." [94]

Surveillance apparatus growing in technical prowess, poses a danger to online activism in Egypt, and has for the most part restricted the once diverse blogosphere and social media activism. Extralegal harassment of mainstream journalists have now extended to online activists, and self censorship has made the Egyptian cyberspace far less lively compared to the Mubarak period.

[6] Direct translation from call to tender, excerpt from Social Networks Security Hazard Monitoring Project Booklet by Egyptian Ministry of Interior

Concluding Observations.

Acceptable Limits of Free Speech

Acceptable limits of expression are vaguely defined, ravaged by numerous limitations and conditions, and at times are almost arbitrarily retracted and burdened by state actors in all but few countries in the region. Most nations in which the conventional media is subject to heavy regulation by the state, citizens have resorted to the internet, especially social media as the single remaining platform which has not completely subdued to political scrutiny.

The use of internet as a utility in disseminating information to the wider public, informing foreign media, mass distribution of politically or culturally volatile content and circumventing the censorship of traditional media has been evident, to both the public and the authorities following Arab Spring.

A trend that is often observed in most authoritarian states in the MENA region is the arbitrary and selective nature of censorship and prosecution, which reveals the tendency of the state to send occasional messages to the wider public to practice self censorship online,(rather than take the financial and technical burden upon themselves to survey and filter content) this practice in some cases has been able to make an impression, but in most others, has further encouraged activists to defy the status quo.

Freedoms within censorship

Surveillance and censorship in MENA regions tend to be multi layered, in a sense of engineering and fine tuning the state apparatus in various degrees to suit various forms of expression and data on the internet. Extreme cases would be Saudi Arabia and Iran, where religion is indistinguishable from the faculties of governance, and the critique of one, is automatically passed as that of the other.

When confronted with a region in the world where the definition of freedom of speech is vague and governed by numerous restrictions peculiar to each nation, studying the tacitly perceived "Red Lines" helps the observer understand with better clarity, the extent of freedom an internet user may enjoy.

For example, Morocco, perceived as being comparatively liberal in the region has tacitly known guidelines in the discussion of the Monarch and the Military. The Prime minister holds the idea that secularism is a threat to Morocco's social fabric, and Sunni Islam is the declared state religion. Conventional media, for the most part are sensitive to the strict cultural guidelines that have transcended generations - yet they are not only tested - but are argued, criticised and for the most part ignored with very little in the way of penalties.

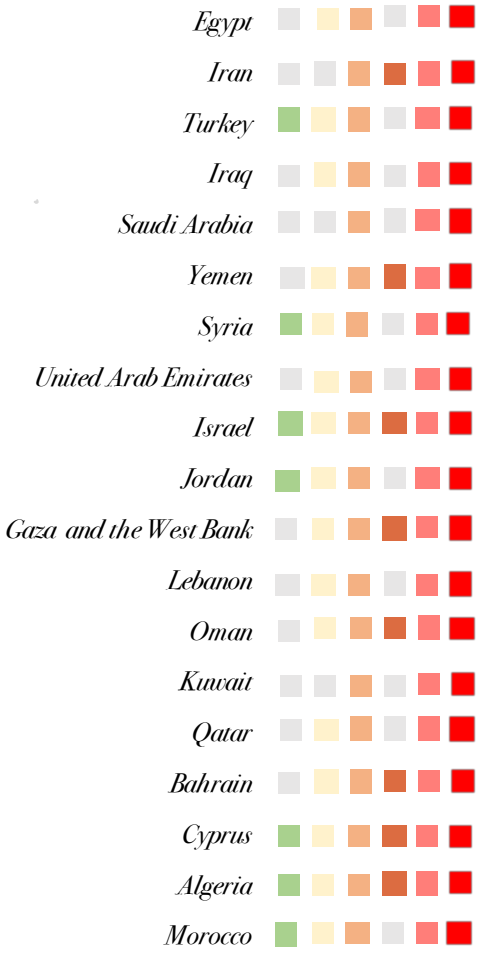
Saudi Arabia and Iran, in a sense have integrated the internet as part of transparent governance, a considerable number of Saudis and Iranians predominantly use the internet to expose low level bureaucratic crimes, unpopular policy, unjust censorship, and reasonably restrained political views. This culture of internet induced people journalism has in many ways aided the transparency and emphasised the few democratic qualities that the governments can offer.

Saudi Arabia has seen an emergent culture of young YouTube content producers, who in ways subtle and mildly sarcastic - engage in soft criticism of generally unpopular government officials, due to the popularity of the content producers, and the inability to affect content production directly, most officials have learned to make space for their critics.

Owing to increased penetration rates, better internet speeds and the transformation of key MENA economies from being Crude centric to Information centric will inevitably result in the expansion of Internet Freedoms in the Arab World. Following the patterns both consistently observed in the MENA regions and particularly the rest of the wold, the state surveillance apparatus will continue to operate, and improve in complexity to accommodate the growing number of users and to tackle the rising cybercrime in the MENA region. However the state of censorship is heavily subjected to the political volatilities of the region, as observed in Libya, Egypt and Iran, yet given that the region continues along a politically non volatile trajectory, especially Iran - as a general rule, the censorship apparatus will become more and more flexible with albeit with intermittent calamities.

Red Lines

Where markers available, denote relatively consistent freedoms enjoyed by the users of social media. Arrests, Censorship and Intimidation of internet users are set to grey markers.



- Religious dissidence, and online presence of religious minorities
- Discussion of Taboo Subjects and sexuality
- Discussion of the social order, or the status quo
- Activism for political opposition, or against prevalent administration
- Suggestions of minor, regional administrative reforms
- Criticism of bureaucracy and corruption in lower Levels of public office
- Censorship, Arrest, Intimidation or self Censorship

[SeeAppendix article 5]

The surveillance climate in the Five Eyes Alliance* is not exempt from criticism either, PEN American Centre's 2015 study, Global Chilling, based on a survey of nearly 800 writers worldwide, demonstrated that concern about mass surveillance is now nearly as high among writers living in democracies (75%) as among those living in non-democracies (80%). The levels of self-censorship reported by writers living in democratic countries are approaching the levels reported by writers living in authoritarian or semi-democratic countries.

Surveillance has put the religious minorities in Iran and Saudi Arabia under pressure, any online congregation or expression of faith is extremely carefully worded - self censorship is highly prevalent among minorities in countries with extremely high censorship.

Women's rights, or at least the discussion thereof has been vastly improved, and continues to improve as a result of online activism despite heavy censorship.

While the fact remains true that surveillance generally does impede civil liberties universally, surveillance with the explicit purpose of mass censorship, the lack of a democratic debate, disregard for human rights, a culture of political impunity and a complete lack of political transparency has put most nations in the Arab World far beyond justifiable parallels to the modus operandi of their western counterparts.

A volatile, gestative research environment.

The collective internet freedoms in the Arab world could be compared to a bubble, which expands and contracts in response to the political situation of the country.

This extreme sensitivity of the cyberspace to the prevalent political situation springs from autocratic power structures being able to pass new laws, change interpretations of legislature, or whimsically redefine religious constraints with very little democratic discourse or due process.

In the long run, this bubble will ultimately expand, growing penetration levels and the enthusiasm in

the Arab world to experience democratic discourse will definitely have an effect on its expansion. The transfer to a completely sovereign cyberspace as threatened by the likes of Iran and Bahrain quite unlikely.

Appendix

-Article 1

All data acquired from ITU (Penetration Rate) and Freedom House Scores (Internet Freedom Rating), Where details are not available, countries are classified with journalistic evidence

Obtained From Freedom House (2014 - 2015)

	Penetration (%)	FIW	FOI	FOI	
Egypt	50	5.5	61	6.1	
Iran	39	6	87	8.7	
Turkey	51	3.5	58	5.8	
Iraq	11.3	6	*	[N/A]	
Saudi Arabia	63	7	73	7.3	
Yemen	22.6	6	*	[N/A]	[1]
Syria	28	7	87	8.7	
United Arab Emira	90	6	68	6.8	
Israel	71.5	1.5	*	[N/A]	[2]
Jordan	44	5.5	50	5	
Palestine[5]	48	5.5	*	[N/A]	[3]
Lebanon	74.7	4.5	45	4.5	
Oman	70	5.5	*	[N/A]	[4]
Kuwait	78	5	*	[N/A]	[5]
Qatar	91	5.5	*	[N/A]	[6]
Bahrain	91	6.5	72	7.2	
Cyprus	70	1	*	[N/A]	[7]

[1] Internetsociety.org and igmena.org has extensively documented Yemen
[2] Times of Israel Carries a list of articles related to internet freedom in Israel
[3] Internet Freedom In the Gaza Strip and the WestBank
[4] ONI offers information on Gaza and the Westbank, Only partly free due to extnsive surveilance
[5] Human Rights Watch and US State department cites heavy censorship, and violation of user rights
[6] ONI offers information on Qatar, cites pervasive filtering and censorship
[7] Freedom in the World, and Press Freedom reflects a free and open internet, surveilance, as revealed by ONI is selective.

Obtained From Open Net Initiative

-Article 2

AE	United Arab Emirates	3	substantial	4	pervasive	4	pervasive	2	selective	Medium	High	2009
AZ	Azerbaijan	2	selective	2	selective	0	no evidence	0	no evidence	Low	Low	2008
BH	Bahrain	4	pervasive	4	pervasive	3	substantial	2	selective	Medium	High	2009
EG	Egypt	0	no evidence	0	no evider	0	no evidence	0	no evidence	n/a	n/a	2012
IL	Israel	0	no evidence	0	no evider	0	no evidence	0	no evidence	n/a	n/a	2009
IQ	Iraq	0	no evidence	0	no evider	0	no evidence	0	no evidence	n/a	n/a	2009
IR	Iran	4	pervasive	4	pervasive	4	pervasive	3	substantial	Medium	High	2011
JO	Jordan	2	selective	0	no evider	0	no evidence	0	no evidence	Medium	Low	2009
KW	Kuwait	2	selective	4	pervasive	4	pervasive	2	selective	Medium	Medium	2009
LB	Lebanon	0	no evidence	0	no evider	0	no evidence	0	no evidence	n/a	n/a	2009
LY	Libya	2	selective	0	no evider	0	no evidence	0	no evidence	n/a	n/a	2009
MA	Morocco	0	no evidence	2	selective	2	selective	2	selective	Low	Medium	2009
OM	Oman	2	selective	4	pervasive	3	substantial	0	no evidence	Medium	High	2009
PS	Gaza and the West Bank	0	no evidence	3	substanti	0	no evidence	0	no evidence	Low	Medium	2009
SA	Saudi Arabia	3	substantial	4	pervasive	4	pervasive	2	selective	High	High	2009
SY	Syria	4	pervasive	2	selective	4	pervasive	2	selective	Low	High	2009
TN	Tunisia	0	no evidence	0	no evider	0	no evidence	0	no evidence	n/a	n/a	2012
TR	Turkey	2	selective	2	selective	2	selective	0	no evidence	Medium	Low	2010
YE	Yemen	3	substantial	4	pervasive	3	substantial	2	selective	Medium	High	2012

-Article 3
All sources are detailed in the Freedom House reports in their respective years.

(1) Content Refinery, mentioned in the graphic refers to an advanced censorship and filtration system that was planned to be a part of Iranian National Internet, which attempted to sanitise the content of any information that deemed to harm the Social Order of Iran, There is no evidence that this plan is pursued by the current Hassan Rouhani regime in the same extent.

-Article 4

All sources are detailed in the Freedom House reports in their respective years.

(1) Saudi Anti terror regulations, mentioned herein, are referred to in the Bibliography

[13] https://www.hrw.org/news/2014/03/20/saudi-arabia-new-terrorism-regulations-assault-rights : Saudi interior ministry regulations include other sweeping provisions that authorities can use to criminalise virtually any expression or association critical of the government and its understanding of Islam. These "terrorism" provisions include the following: Article 1: "Calling for atheist thought in any form, or calling into question the fundamentals of the Islamic religion on which this country is based."

-Article 5

The red lines, or the taboo subjects are determined by the analysis of Freedom house reports, with regards to reported instances where internet users have faced consequences for approaching the subject(s) online/ or maintain self censorship. Of course, the chart tends to generalise - and no too instances are the same, but the idea is to paint a brief picture as to what limitations for content are generally imposed upon internet users in the respective countries.

Reference List :

[40] [41] [42] Saudi Arabia Profile - Media (2015) Available From : http://www.bbc.co.uk/news/world-middle-east-14703480 (2015)

Why Twitter is so big in Saudi Arabia : Available From : http://www.bbc.co.uk/news/blogs-trending-25864558 [Last Accessed 25th March 2016)]

[65] A Warning to Know Your Customer: Computerlinks Fined for Dealing Blue Coat Surveillance Technology to Syria: Available From : https://www.eff.org/deeplinks/2013/05/blue-coat-syria-scandal-next-shoe-drops-computerlinks-fzc0 [Last Accessed 26th March 2016)]

[68] A compilation of basic documents by wassenaar.org (2016) , highlights basic criteria for responsible sale of surveillance equipment Available From : http://www.wassenaar.org/wp-content/uploads/2016/01/WA-DOC-16-SEC-001-Basic-Documents-2016-January.pdf

[69] Explaining the Intensity of the Arab Spring Chonghyun Christie Byun, PhD Wabash College Ethan J. Hollander, PhD Wabash College (Published Spring 2015, Accessible via http://onlinelibrary.wiley.com.chain.kent.ac.uk/doi/10.1111/dome.12057/epdf)

[72] Gholam Khiabany (2015). Technologies of Liberation and/or Otherwise. International Journal of Middle East Studies, 47, pp 348-353.

[78]Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA: Available From : https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa [Last Accessed 31th March 2016)]

[84] Egypt Leaves the Internet (2011) : Available From http://research.dyn.com/2011/01/egypt-leaves-the-internet/ [Last Accessed 30th March 2016)]

[94] Administrative Court Lawsuit: Stop Social Media Surveillance in Egypt : Available From : https://advox.globalvoices.org/2014/06/19/administrative-court-lawsuit-to-stop-social-media-surveillance-in-egypt/[Last Accessed 29th March 2016)]

Bibliography :

[1] A Magna Carta of the Internet : https://webwewant.org http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

[2] Arguments and criticisms of a Magna Carta for the world wide web http://www.computerweekly.com/opinion/A-digital-Magna-Carta-is-Tim-Berners-Lee-on-the-right-track

Why an Internet Bill of Rights will Never Work http://www.techrepublic.com/article/why-an-internet-bill-of-rights-will-never-work-and-whats-more-important/

[3] igMena is a consortium of online activists in the region : http://igmena.org/about Seeds of the future : Online activism in the Middle East http://www.economist.com/blogs/newsbook/2012/05/online-activists-middle-east

[4] Political Oppression of Internet Activists well Documented in igMena reports, Freedom House, Reporters without Borders and Human

[6] Draft Investigatory Powers Bill : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf Draft Investigatory Powers Bill : Edward Snowden Attacks http://www.theguardian.com/world/2015/nov/04/edward-snowden-attacks-tories-over-investigatory-powers-bill

[7] Politically Volatile Countries : Documented in https://www.freedomhouse.org/report/middle-east-and-north-africa-fact-sheet#.UuDsNRA051t Freedom House Middle East and North Africa Fact Sheet

[8] Manual for Measuring ICT Access and Use by Households and Individuals, 2014http://www.itu.int/en/ITU-D/Statistics/Pages/publications/manual2014.aspx

[9] Referring to cases such as Iran, obtaining information directly from authorities may not always paint the right picture : Statistics on the number of internet users in Iran are inconsistent and highly disputed, though most observers agree that usage continues to grow. According to the National Internet Development Management Center (MATMA), the national internet penetration rate was 49 percent in 2014-15, which is lower than the figure of 61 percent that was reported by the same agency one year ago : Freedom House - Iran, Obstacles to access

[10]http://vc.bridgew.edu/cgi/viewcontent.cgi?article=1004&context=jiws Arab Women, Social Media, and the Arab Spring: Applying the framework of digital re exivity to analyze gender and online activism Victoria A. Newsom Lara Lengel (Oct 2012)

[11] David Romano, "Modern Communications Technology in Ethnic Nationalist Hands: The Case of the Kurds," *Canadian Journal of Political Science*, Vo. 35, No. 1 (2002): 127-149.

[13] https://www.hrw.org/news/2014/03/20/saudi-arabia-new-terrorism-regulations-assault-rights : Saudi interior ministry regulations include other sweeping provisions that authorities can use to criminalise virtually any expression or association critical of the government and its understanding of Islam. These "terrorism" provisions include the following: Article 1: "Calling for atheist thought in any form, or calling into question the fundamentals of the Islamic religion on which this country is based."

[15] http://www.al-monitor.com/pulse/ar/culture/2012/12/blogging-in-the-arab-world.html : Also well documented in Freedom House and Human Rights Watch Reports

[16]Syria, Online Tracking : http://12mars.rsf.org/2014-en/2014/03/11/syria-online-tracking-is-a-family-affair/ http://12mars.rsf.org/2014-en/2014/03/11/iran-the-revolutionary-guards-the-supreme-council-for-cyberspace-and-the-working-group-for-identifying-criminal-content/ http://12mars.rsf.org/2014-en/2014/03/11/saudi-arabia/ http://12mars.rsf.org/2014-en/2014/03/11/bahrain-no-internet-spring/

[17] Based on ITU figures for online penetration, Freedom House Figures and ONI for internet freedom and political status, and reporters without borders enemies of the internet report (http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf)

[18] Largely based on ONI figures : Refer Appendix Extension 2

[19]

[20] [21] [22] [23] [24]
Journal of Information Technology, 2010, Vol. 25(2),p244 [Peer Reviewed Journal]
Conviviality of Internet social networks:
An exploratory study of Internet campaigns in Iran
Aghil Ameripour1
, Brian Nicholson1
, Michael Newman1,2

[25] Iran internet law sparks suspicion (Al Jazeera 2009) http://www.aljazeera.com/news/middleeast/2009/07/200972013283267852 5.html

[26]

[27] https://freedomhouse.org/report/freedom-net/2011/iran Still banned : http://america.aljazeera.com/opinions/2014/4/iran-twitter-rouhaniinternetcensorship.html

[28] [29] [30] [31] (Content Removed)

[32] Grand Ayatollah Declares High Speed Internet Haram : https://www.iranhumanrights.org/2014/08/makarem-internet/

[33] [34] Freedom House : https://freedomhouse.org/report/freedom-net/2015/iran

[35] Iranian Minister of Culture, Al Jazeera Interview on Social mediahttps://www.youtube.com/watch?v=6rgPqFL4aJg (20:45 Minutes onwards)

[36] Netflix opens up in Iran : https://www.iranhumanrights.org/2016/01/netflix-filtered/

[37] Iran's National SSL certification https://www.iranhumanrights.org/2014/11/internet-report-national-ssl-certificates/

[38] Freedom House : https://freedomhouse.org/report/freedom-net/2015/iran

[39] Iran's Startup Scene : http://www.bbc.co.uk/news/world-middle-east-34458898 http://www.huffingtonpost.com/elnaz-moghangard/iran-the-next-startup-hub_b_8583584.html

[43] https://www.hrw.org/news/2014/02/06/saudi-arabia-terrorism-law-tramples-rights

[45] [46] [47] [48] [48] (Content Removed)

[44] [50, 53] [59] Mass surveillance on social media, Saudi Arabia : Freedom House : https://freedomhouse.org/report/freedom-net/2015/saudi-arabia

[52]hacking team saudi arabia : http://www.theregister.co.uk/2015/09/28/saudi_arabia_hacking_team/

[54] Saudi Arabia and NSA : Snowden Memo : https://theintercept.com/document/2014/07/25/saudi-arabia-information-paper/ From Glenn Greenwald's article from The Intercept https://theintercept.com/2014/07/25/nsas-new-partner-spying-saudi-arabias-brutal-state-police/

[55] [58] [60] [56] (Content Removed)

[57] Saudi Arabia: Terrorism Law Targets Peaceful Speech
'Insulting State's Reputation' Among New 'Terrorism' Offenses https://www.hrw.org/news/2013/12/30/saudi-arabia-terrorism-law-targets-peaceful-speech

[62] http://www.scmp.com/tech/enterprises/article/1921929/zte-faces-us-export-restrictions-over-iran-surveillance-system-deal

[63] http://www.bloomberg.com/news/articles/2011-12-23/israel-didn-t-know-high-tech-gear-was-sent-to-iran-via-denmark

[64] https://www.bluecoat.com/company/news/update-blue-coat-devices-syria

[66] (Content Removed)
[67] https://edri.org/edrigramnumber10-10amesys-complicity-in-torture/

[71] Refer Appendix

[74] [75] [76] https://freedomhouse.org/report/freedom-net/2010/tunisia and /2011/tunisia

[80] [81] [82] /2013/tunisia

[77] https://opennet.net/research/profiles/tunisia

[83] https://freedomhouse.org/report/freedom-net/2011/egypt

[85] [86] (Content Removed)

[87] [89] [92] [93] https://freedomhouse.org/report/freedom-net/2015/egypt

[88] http://gulfnews.com/news/mena/egypt/egyptian-blogger-first-to-win-award-1.197536

[91] [89] https://freedomhouse.org/report/freedom-net/2013/egypt